**МРНТИ 27.41.15**
**УДК 511.214**

**10.51889/2959-5894.2023.83.3.007**

*У.К. Турусбекова[1*], М.М. Муратбеков[2], С.А. Алтынбек[3], Ж.Е. Ахатова[4]*

*[1]Учреждение «Esil University», г. Астана, Казахстан*
*[2]Евразийский национальный университет им. Л.Н. Гумилева, г. Астана, Казахстан*
*[3]Казахский университет технологии и бизнеса, г. Астана, Казахстан*
*[4]Казахский национальный женский педагогический университет, г. Алматы, Казахстан*
*[*]e-mail: umut.t@mail.ru*

# ИССЛЕДОВАНИЕ СВОЙСТВ СТРУКТУР РЕКУРСИВНЫХ ЦИКЛОВ ПЕРВООБРАЗНЫХ КОРНЕЙ

*Аннотация*

Решение многих задач современной теории простых чисел позволяет, с одной стороны, углубить представление о том, как развивать фундаментальные основы математики, а с другой - создавать более эффективные арифметические методы построения быстрых алгоритмов или дискретных ортогональных преобразований при анализе и обработке сложных данных. Одной из проблем современной математики в совокупности с криптографией является задача поиска первообразных (примитивных) корней. В данной статье рассмотрена задача вычисления множества всех первообразных корней произвольного простого числа p. Кроме того, описана важность данной задачи в современном мире, в частности, использование теории первообразных корней в криптографии. Построен алгоритм проверки натурального числа n на свойство быть первообразным корнем заданного простого числа. В ходе работы установлено, что существуют неспецифические рекурсивные циклы, исследованы свойства структур рекурсивных циклов первообразных корней. Доказано, что все первообразные корни любого простого числа образуют пары, в которых рекурсивный цикл одного является инверсией рекурсивного цикла другого элемента пары. Приведены примеры первообразных корней и их внутренних циклов, а также инверсионные пары. Данное свойство примитивных корней не отмечалось ранее в литературе. В ходе работы также исследованы возможности представления рекурсивных циклов в двумерном пространстве. Результаты представлены в виде графиков инверсионных пар первообразных корней простых чисел. Показано, что рекурсивные циклы образуют динамические процессы. Доказано, что динамические процессы имеют хаотический характер, исследование которого является важной задачей теории динамических систем. В дальнейшем планируется детально исследовать структуру внутренних циклов для пар чисел. Анализ таких структур является шагом к решению сложных теоретико–математических задач и задач криптографии, где используются примитивные корни.

**Ключевые слова**: примитивный корень, циклическая группа, группа перестановок, простое число, рекурсивный цикл.

*Аңдатпа*

*У.К. Турусбекова[1], М.М. Муратбеков[2], С.А. Алтынбек[3], Ж.Е. Ахатова[4]*
*[1]«Esil University» мекемесі, Астана, Қазақстан*
*[2]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан*
*[3]Қазақ технология және бизнес университеті, Астана, Қазақстан*
*[4]Қазақ ұлттық қыздар педагогикалық университеті, Алматы, Қазақстан*

# АЛҒАШҚЫ ТҮБІРЛЕРДІҢ РЕКУРСИВТІ ЦИКЛ ҚҰРЫЛЫМДАРЫНЫҢ ҚАСИЕТТЕРІН ЗЕРТТЕУ

Қазіргі жай сандар теориясының көптеген мәселелерін шешу, бір жағынан, математиканың іргелі негіздерін қалай дамыту керектігі туралы идеяны тереңдетуге, екінші жағынан, күрделі деректерді талдау және өңдеу кезінде жылдам алгоритмдерді немесе дискретті ортогональды түрлендірулерді құрудың тиімді арифметикалық әдістерін жасауға мүмкіндік береді. Қазіргі математика мен криптография проблемаларының бірі-алғашқы (примитивті) түбірлерді табу есебі болып табылады. Ұсынылған мақалада кездейсоқ p жай санының барлық алғашқы түбірлері жиынтығын есептеу есебі қарастырылған. Сонымен қатар, қазіргі әлемде бұл мәселенің маңыздылығы, атап айтқанда криптографияда алғашқы түбірлер теориясын қолдану мәселелері сипатталған. Берілген жай санның алғашқы түбірі болу қасиетіне n натурал санды тексеру алгоритмі құрылды. Жұмыс барысында спецификалық емес рекурсивті циклдар бар екендігі анықталды, алғашқы түбірлердің рекурсивті циклдерінің құрылымдарының қасиеттері зерттелді. Кез-келген жай санның барлық алғашқы түбірлері жұптарды құрайтындығы дәлелденді, онда біреуінің рекурсивті циклі жұптың басқа элементінің рекурсивті циклінің инверсиясы болып табылады. Қарапайым түбірлер мен олардың ішкі циклдерінің мысалдары, сондай-ақ инверсиялық жұптар келтірілген. Алғашқы түбірлердің бұл қасиеті бұрын әдебиетте атап өтілмеген. Жұмыс барысында екі өлшемді кеңістіктегі рекурсивті циклдерді ұсыну мүмкіндіктері де зерттелді. Нәтижелер

қарапайым сандардың алғашқы түбірлерінің инверсиялық жұптарының графигі түрінде ұсынылған. Рекурсивті циклдер динамикалық процестерді құрайтыны көрсетілген. Динамикалық процестер хаотикалық сипатқа ие екендігі дәлелденді, оны зерттеу динамикалық жүйелер теориясының маңызды есебі болып табылады. Болашақта жұп сандар үшін ішкі циклдердің құрылымын егжей-тегжейлі зерттеу жоспарлануда. Мұндай құрылымдарды талдау күрделі теориялық және математикалық есептер мен алғашқы түбірлер қолданылатын криптография есептерін шешуге қадам болып табылады.

**Түйін сөздер:** алғашқы түбір, циклдік топ, орын ауыстыру тобы, жай сан, рекурсивті цикл.

*Abstract*

**INVESTIGATION OF THE PROPERTIES OF RECURSIVE CYCLES STRUCTURES OF PRIMITIVE ROOTS**

*TurusbekovaU.K. [1], Muratbekov M.M. [2], Altynbek S.A. [3], Akhatova Zh.E. [4]*
*[1]Institution "Esil University", Astana, Kazakhstan*
*[2]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan*
*[3]Kazakh University of Technology and Business, Astana, Kazakhstan*
*[4]Kazakh National Women's Pedagogical University, Almaty, Kazakhstan*

Solving many problems of the modern theory of prime numbers allows, on the one hand, to deepen the understanding of how to develop the fundamental foundations of mathematics, and on the other - to create more effective arithmetic methods for constructing fast algorithms or discrete orthogonal transformations in the analysis and processing of complex data. One of the problems of modern mathematics in combination with cryptography is the problem of finding primitive roots. This article considers the problem of calculating the set of all primitive roots of an arbitrary prime number p. In addition, the importance of this task in the modern world is described, in particular, the use of the theory of primitive roots in cryptography. An algorithm for checking the natural number n for the property of being a primitive root of a given prime number is constructed. During the work it was found that there are non-specific recursive cycles, the properties of the structures of recursive cycles of primitive roots were investigated. It is proved that all primitive roots of any prime number form pairs in which the recursive cycle of one is an inversion of the recursive cycle of the other element of the pair. Examples of primitive roots and their inner cycles, as well as inversion pairs are given. This property of primitive roots has not been noted before in the literature. In the course of the work, the possibilities of representing recursive cycles in two-dimensional space are also investigated. The results are presented in the form of graphs of inversion pairs of primitive roots of prime numbers. It is shown that recursive cycles form dynamic processes. It is proved that dynamic processes have a chaotic character, the study of which is an important task of the theory of dynamical systems. In the future, it is planned to study in detail the structure of internal cycles for pairs of numbers. The analysis of such structures is a step towards solving complex theoretical and mathematical problems and cryptography problems where primitive roots are used.

**Keywords:** primitive root, cyclic group, permutation group, prime number, recursive cycle.

**Введение**

В современной как фундаментальной, так и прикладной математике теория простых чисел обладает исключительной привлекательностью. Решение многих проблем современной теории простых чисел позволяет, с одной стороны, углубить представление о том, как развивать фундаментальные основы математики, а с другой стороны, позволит создавать все более эффективные арифметические методы для построения быстрых алгоритмов дискретных ортогональных преобразований в анализ и обработка сложных данных [1]. К сложным данным относится современная эра науки о больших данных [2], обработки сигналов, криптографии [3] и других.

Опыт работы над проблемами фундаментальной и прикладной математики показывает, что существуют нерешенные математические задачи, решение которых важно, как для углубления и разработки новых методов решения сложных задач фундаментальной математики, так и для создания эффективных алгоритмов решения задач из прикладных областей, некоторые из которых перечислены выше.

До сих пор не доказана справедливость гипотезы Артина [4], согласно которой, если натуральное число не равно 0, ±1 и является совершенным квадратом, то имеет место равенство

$$\pi(x,a) = c(a)\cdot\pi(x), \tag{1}$$

где $\pi(x,a)$ - число простых чисел, $\pi(x)$ - число простых чисел, для которых $x$ является примитивным корнем, $c(a)$ – константа, зависящая только от значения $a$.

В работе [5] сформулирована обобщенная гипотеза Артина, а также определены способы ее решения с помощью экспериментальной математики [6, 7]. Безусловно, любые результаты, полученные на основе компьютерного моделирования, должны быть дополнительно подтверждены аналитическими методами [8,9].

Простое привлечение аналитических методов для решения этой гипотезы Артина и ее обобщения на данный момент невозможно. Существование константы $c(a)$ в (1) подтверждает простое рассуждение, а именно, что должна существовать процедура регулярного сдвига простых чисел для любого числа, для которого $a$ является примитивным корнем. В работе [10] доказано, что таких простых чисел бесконечно много. До сих пор не было доказано, какими свойствами обладают все простые числа, для которых $a$ является примитивным корнем, то есть $a$ является порождающим элементом циклической группы $\left(Z / Z_p\right)^*$ для любого $p \in P$, где $P$ - множество всех простых чисел [11].

Чтобы решить эту проблему, имеет смысл изначально решить другую, как нам кажется, более простую задачу. Для некоторого простого числа $p$ найти все его первообразные корни и изучить их свойства.

Очевидно, что если $a$ является корнем примитивного числа, то достаточно рассмотреть $a < p$. В общем случае число $a$ может быть составным, но не ±1 и идеальным квадратом. Известно, что для любого $p$ число его примитивных корней равно $\varphi(p-1)$, где $\varphi$ – функция Эйлера. С увеличением $p$ число примитивных корней увеличивается. Пусть $m_i$ - некоторый примитивный корень из простого числа $p$. Пусть, $m_p = \{m_{1p}, m_{2p}, ..., m_{\varphi(p-1)p}\}$ - множество всех примитивных корней простого числа $p$. Потенциально, примитивными корнями простого числа $p$ могут быть любые числа от 2 до $p-1$, за исключением тех, которые являются идеальными квадратами.

Проверка числа $m$ на возможность того, что оно является примитивным корнем простого числа $p$, является вычислительно сложной с алгоритмической точки зрения, если принять во внимание, что количество проверок увеличивается с увеличением $p$. Кроме того, для любого простого числа вычисление функции Эйлера $\varphi(p-1)$, которая определяется следующим выражением, является непростой задачей:

$$\varphi(p-1) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_{i-1}}\right), \tag{2}$$

где $p-1 = \prod_{i=1}^{k} p_i^{\alpha_i}$ - его простая факторизация. Вычисление самой функции Эйлера является вычислительно простой задачей. Гораздо более сложной проблемой является разложение на множители числа $p-1$. Если $p-1$ небольшое число, например порядка $10^6$, то задача факторизации решается довольно просто. При значительно более высоких значениях возникают вычислительные трудности подэкспоненциального характера. Для решения задачи факторизации были использованы методы, описанные в [11].

**Методы исследования**

Согласно теореме Ферма, если число $m$ является первообразным корнем из числа $p$, то выполняется условие

$$m^{p-1} \equiv 1 (\mathrm{mod}\, p). \tag{3}$$

Это условие необходимо, но недостаточно. По этой причине необходимо выполнить проверку по более сложной процедуре, приведенной в монографии [11]. Пусть задано простое число $p$, а кандидатом на примитивные корни является $m$. Мы выполняем факторизацию $p-1$, представляя $p-1 = \prod_{i=1}^{k} p_i^{\alpha_i}$, и для каждого простого множителя из $\{p_1, p_2, ..., p_k\}$ проверяем условие

$$m^{\frac{p-1}{p_i}} \equiv 1 (\mathrm{mod}\, p). \tag{4}$$

Для этого реализуется рекурсивная процедура

$$x_{n+1} = mx_n (\mathrm{mod}\, p), \tag{5}$$

от $x_0 = 1$ до $n+1 = \dfrac{p-1}{p_i}$ и вышеупомянутое условие (4) должно быть выполнено на последнем шаге рекурсии.

Предположим, что для некоторого числа выполняется условие (4), тогда мы вычисляем последовательность значений

$$x_p = 1,\ x_{n+1} = mx (\mathrm{mod}\, p) \text{ до } x_{p-1} \equiv 1 (\mathrm{mod}\, p) \tag{6}$$

и мы получаем вектор $\left(x_{1\cdot m_1}, x_{2\cdot m_1}, ..., x_{(p-1)\cdot m_1}\right)$ длины $p-2$. Такие векторы строятся для всех

$$m_i \in m_p = \left\{m_{1\cdot p}, m_{2\cdot p}, ..., m_{(p-1)p}\right\}. \tag{7}$$

Очевидно, что для всех примитивных корней множества *m* все векторы имеют одинаковую длину, равную $p-2$. Множество таких векторов является основой для анализа свойств множества примитивных корней простого числа *p*. Отметим, что цикл рекурсии для примитивного корня $m_i$ на самом деле имеет вид:

$$\left(1, x_{2\cdot m_i}, ..., x_{(p-1)\cdot m_i}\right). \tag{8}$$

Последняя единица относится к следующему циклу, и поэтому длина цикла равна $p-1$, что согласуется с малой теоремой Ферма [12]. Анализ циклов (орбит) рекурсий для множества всех примитивных корней позволил нам установить, что для любого $m_{i\cdot p} \in \left\{m_{1\cdot p}, m_{2\cdot p}, ..., m_{\varphi(p-1)p}\right\}$ всегда существует $m_{j\cdot p}$ при $j \neq p$, что рекурсивный цикл $m_{i\cdot p}$ без первой единицы является инверсией из цикла $m_{j\cdot p}$. По сути, множество $\left\{m_{1\cdot p}, m_{2\cdot p}, ..., m_{\varphi(p-1)p}\right\}$ разлагается на пары примитивных корней. Это - новое свойство множества примитивных корней, которое ранее не было известно. Число примитивных корней является наибольшим для простых чисел $p^* = Z_p + 1$ для $p^* \cdot p \in P$, которые обычно называют простыми числами Софи Жермен и наименьшим числом гладких простых чисел [11]. Для различных $p \in P$ число составных примитивных корней всегда значительно больше, чем число простых примитивных корней. Это объясняется достаточно просто, поскольку $\varphi(p-1)$ показывает количество натуральных чисел, которые являются относительно простыми по отношению к $p-1$.

Каждый примитивный корень является предком для группы $\left(Z / Z_p\right)^*$. Кроме того, каждый из них генерирует набор псевдослучайных чисел. Если мы усредним по множеству всех циклов, то получим псевдослучайную последовательность, в которой все тесты на случайность позволяют утверждать, что в этой последовательности нет внутренних циклов в какой-либо форме.

**Результаты исследования**

Рассмотрим примитивные корни и циклы для простого числа *p* = 37.

*Таблица 1. Обратный рекурсивный цикл примитивных корней 2 и 19 простого числа 37*

| *Примитивный корень* | *Цикл* |
|---|---|
| *2* | *2, 4, 8, 16, 32, 27, 17, 34, 31, 25, 13, 26, 15, 30, 23, 9, 18, 36, 35, 33, 29, 21, 5, 10, 20, 3, 6, 12, 24, 11, 22, 7, 14, 28, 19, 1* |
| *19* | *19, 28, 14, 7, 22, 11, 24, 12, 6, 3, 20, 10, 5, 21, 29, 33, 35, 36, 18, 9, 23, 30, 15, 26, 13, 25, 31, 34, 17, 27, 32, 16, 8, 4, 2, 1* |

*Таблица 2. Обратный рекурсивный цикл примитивных корней 5 и 15 простого числа 37*

| *Примитивный корень* | *Цикл* |
|---|---|
| *5* | *5, 25, 14, 33, 17, 11, 18, 16, 6, 30, 2, 10, 13, 28, 29, 34, 22, 36, 32, 12, 23, 4, 20, 26, 19, 21, 31, 7, 35, 27, 24, 9, 8, 3, 15, 1* |
| *15* | *15, 3, 8, 9, 24, 27, 35, 7, 31, 21, 19, 26, 20, 4, 23, 12, 32, 36, 22, 34, 29, 28, 13, 10, 2, 30, 6, 16, 18, 11, 17, 33, 14, 25, 5,1* |

*Таблица 3. Обратный рекурсивный цикл примитивных корней 13 и 20 простого числа 37*

| Примитивный корень | Цикл |
|---|---|
| 13 | 13, 21, 14, 34, 35, 11, 32, 9, 6, 4, 15, 10, 19, 25, 29, 7, 17, 36, 24, 16, 23, 3, 2, 26, 5, 28, 31, 33, 22, 27, 18, 12, 8, 30, 20, 1 |
| 20 | 20, 30, 8, 12, 18, 27, 22, 33, 31, 28, 5, 26, 2, 3, 23, 16, 24, 36, 17, 7, 29, 25, 19, 10, 15, 4, 6, 9, 32, 11, 35, 34, 14, 21, 13, 1 |

*Таблица 4. Обратный рекурсивный цикл примитивных корней 17 и 24 простого числа 37*

| Примитивный корень | Цикл |
|---|---|
| 17 | 17, 30, 29, 12, 19, 27, 15, 33, 6, 28, 32, 26, 35, 3, 14, 16, 13, 36, 20, 7, 8, 25, 18, 10, 22, 4, 31, 9, 5, 11, 2, 34, 23, 21, 24, 1 |
| 24 | 24, 21, 23, 34, 2, 11, 5, 9, 31, 4, 22, 10, 18, 25, 8, 7, 20, 36, 13, 16, 14, 3, 35, 26, 32, 28, 6, 33, 15, 27, 19, 12, 29, 30, 17, 1 |

*Таблица 5. Обратный рекурсивный цикл примитивных корней 18 и 35 простого числа 37*

| Примитивный корень | Цикл |
|---|---|
| 18 | 18, 28, 23, 7, 15, 11, 13, 12, 31, 3, 17, 10, 32, 21, 8, 33, 2, 36, 19, 9, 14, 30, 22, 26, 24, 25, 6, 34, 20, 27, 5, 16, 29, 4, 35, 1 |
| 35 | 35, 4, 29, 16, 5, 27, 20, 34, 6, 25, 24, 26, 22, 30, 14, 9, 19, 36, 2, 33, 8, 21, 32, 10, 17, 3, 31, 12, 13, 11, 15, 7, 23, 28, 18, 1 |

*Таблица 6. Обратный рекурсивный цикл примитивных корней 22 и 32 простого числа 37*

| Примитивный корень | Цикл |
|---|---|
| 22 | 18, 28, 23, 7, 15, 11, 13, 12, 31, 3, 17, 10, 32, 21, 8, 33, 2, 36, 19, 9, 14, 30, 22, 26, 24, 25, 6, 34, 20, 27, 5, 16, 29, 4, 35, 1 |
| 32 | 35, 4, 29, 16, 5, 27, 20, 34, 6, 25, 24, 26, 22, 30, 14, 9, 19, 36, 2, 33, 8, 21, 32, 10, 17, 3, 31, 12, 13, 11, 15, 7, 23, 28, 18, 1 |

Значение функции Эйлера для этого числа будет равно $\varphi(p-1)=12$, что равно числу примитивных корней для данного простого числа. Как следует из приведенных выше данных (таблицы 1-6), все примитивные корни имеют рекурсивно - обратную пару. На рисунках 1-3 представлены графики инверсионных пар примитивных корней простого числа 37 в двумерной системе.

Фактически, на основе данных о примитивных корнях простого числа складывается следующая модель для изучения множества простых чисел, для которых данное число $a$ является примитивным корнем. Предположим, что выбрано $a$ и установлено, что для некоторого $p$ число $a$ является примитивным корнем. Мы находим множество примитивных корней числа $m_p=\{m_{1\cdot p}, m_{2\cdot p},..., m_{\varphi(p-1)p}\}$ и пусть $a$ принадлежит этому множеству.

Кроме того, пусть некоторое $p^*>a$ также принадлежит $m_p$.

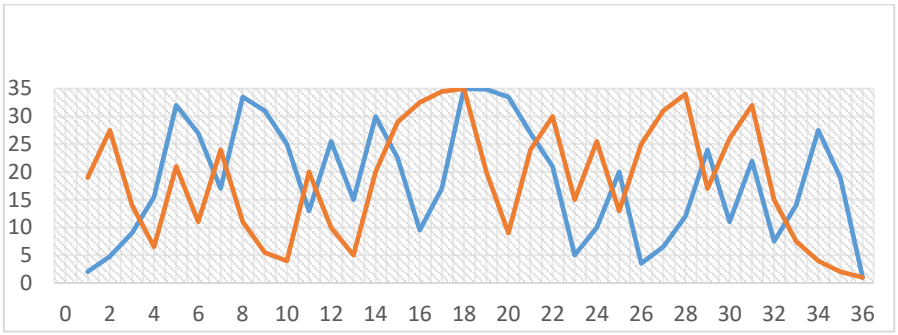


*Рисунок 1. Примитивные корни 2 и 19 простого числа 37 в двумерной системе*

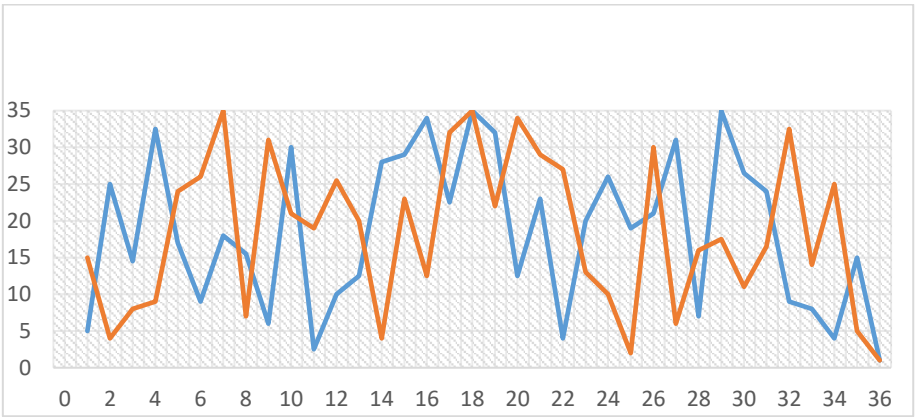


*Рисунок 2. Примитивные корни 5 и 15 простого числа 37 в двумерной системе*

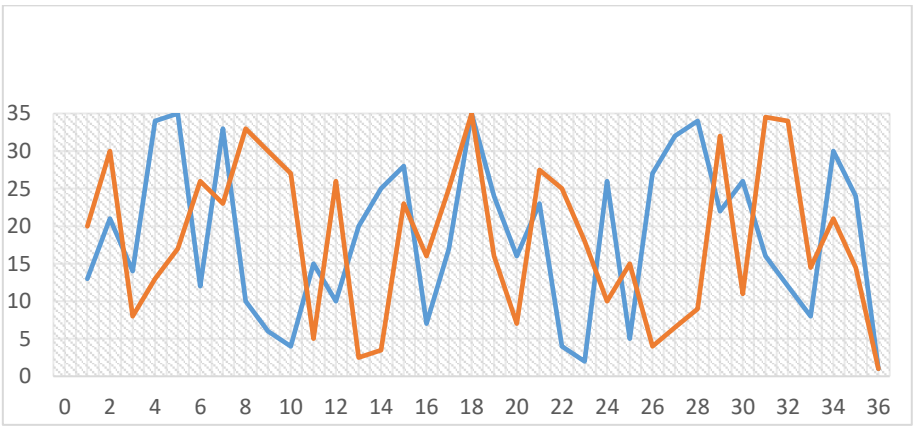


*Рисунок 3. Примитивные корни 13 и 20 простого числа 37 в двумерной системе*

Из анализа экспериментальной математики следует, что $a$ также является первообразным корнем для $p^*$. Таким образом, имеет место схема:

$$a \to p^* \to p \Rightarrow a \to p \tag{9}$$

Если этот переходный "закон" окажется правильным, то появится дополнительная информация о законах формирования множества простых чисел, для которых $a$ является примитивным корнем. Итак, в гипотезе Артина, основанной на данных экспериментальной математики, установлены два факта:

1) для любого $p \in P$ множество

$$m_p = \{m_{1\cdot p}, m_{2\cdot p}, ..., m_{\varphi(p-1)p}\} \tag{10}$$

разделим на пары, в которых рекурсия на основе одного элемента является обратной рекурсии другого элемента пары. Пары могут быть образованы двумя простыми числами, двумя составными числами и одним простым и одним составным. Необходимо доказать этот факт аналитически. Для существования инверсии необходимо и достаточно, чтобы в любой паре $(m_{1\cdot p}, m_{2\cdot p})$ первый элемент рекурсии $m_1$ был равен последнему в $m_2$ и наоборот. Это подразумевает равенство двух рекурсий. Условия, при которых это происходит, вероятно, легко установить. Труднее доказать, что рекурсии совпадают при инверсии.

2) Предположим, что $a$ – примитивный корень для всех $p \in P_a = \{p_1,..., p_a\}$.

Доказать: пусть $a \to p_i$ и $p_i \to p_j = a \to p_i$ при $a < p_i < p_j$, то есть существует транзитивность. Вполне возможно, что это переносится на теорию конечных полей, эллиптических кривых и модулярных форм.

Важный вопрос: как найти модуль $m$ такой, чтобы остатки этого модуля на $P_a$ отличались от остатков этого модуля на множестве а $P - P_a$. Вопрос о существовании такого модуля остается открытым. Возможно, что существует система модулей $\{m_1,..., m_x\}$, остатки над которыми обладают свойствами, определяемыми некоторой функцией типа $f(Z_{ml},..., Z_{mk})$. Это может быть связано с теоремой Дирихле об арифметической прогрессии. Вопрос о том, можно ли его обобщить на систему арифметических прогрессий, остается открытым.

**Заключение**

Анализируя первичные корни, обнаружено, что существуют пары примитивных корней, в которых рекурсия на основе одного элемента является инверсией рекурсии другого элемента пары. Если мы объясним этот момент аналитическим способом, мы получим дополнительную информацию о законах формирования множества простых чисел, для которых $a$ является примитивным корнем. Процессы взаимодействия рекурсивных циклов между различными парами примитивных корней простого числа $p$. Доказано, что динамические процессы имеют хаотическую природу, исследование которой является важной задачей теорий динамических систем.

**Благодарности**

*Работа выполнена при поддержке грантового финансирования по научно-техническим проектам Министерством науки и высшего образования Республики Казахстан, грант № AP19677733.*

*Список использованных источников:*

*1 Чернов, В.М. Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований / В.М. Чернов.- М.: ФИЗМАТЛИТ, 2007.-264 с.*

*2 Mallat, S. Course on High Dimensional Data Analysis / S. Mallat.- École Normale Supérieure, 2013.- 117 p.*

*3 Chakraborty, R. S., Scgwabe, P., Solwaeth, J. (ed.) Security, Privacy and Applied Cryptography Engineering / R.S. Chakraborty, P. Scgwabe, J. Solwaeth // 5th International Conference, SPACE 2015, Jaipur, India, October 3-7, 2015. Proceedings.- Springer , 2015.-V. 9354. - P. 37–42.*

*4 Ambrose D. On Artin's Primitive Root Conjecture. Dissertation zur Erlangung des mathematisch-naturwissenschaftlichen Doctorgrades //Doctor rerum naturalium. – der Georg-August-Universitat Gottingen, 2014. - 169 p.*

*5 Vostrov, G. N., Opjata, R. J. Computer modeling of dynamic processes in analytic number theory / G. N. Vostrov, R. J. Opjata // Електротехнічні та комп'ютерні системи. - 2018. - №.28 (104) - P. 240-247. https://doi.org/10.15276/eltecs.28.104.2018.29.*

*6 Caragiu, M. Sequential Experiments with Primes / M. Caragiu.-Springer International Publishing, 2017.- 290 p.*

*7 Lord N. Experimental mathematics in action, by DH Bailey, JM Borwein, NJ Calkin, R. Girgensohn, DR Luke & VH Moll. Pp. 322. $49.00. 2007. ISBN 978 1 56881 271 7 (AK Peters) //The Mathematical Gazette. – 2009. – V. 93. – №. 528. – P. 564-566. https://doi.org/10.1017/S0025557200185511.*

*8 Murty, M. R. Problems in Analytic Number Theory. - 2nd edition / M.Ram Murty. –New York: Springer Science + Business Media LLC, 2008.-506 p.*

*9 Abdymanapov S.., Turusbekova U., Turginbayeva A., Altynbek S. Research of Irreducible Norm Polynomials Special Type over a Field of Characteristic 2 // IAENG International Journal of Applied Mathematics.-2020.-V.50.-№4.- P.777-782. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85098231325&partnerID=40&md5=5949531a97827669e0d339b00af4b250*

*10 Moree, P. A note on Artin's conjecture / P. Moree // Simon Stevin, 1993.- V.67. -№3.- P. 255–258.*

11 Brudern, J., Godinho, H. On Artin's conjecture, II: Paris of additive Forms /J. Brudern, H. Godinho //Proceedings of the London Mathematical Society. - 2002. - V. 84. – №. 3. – P. 513–538. https: // doi.org/10.1112/S0024611502013588.

12 Манин, Ю.И. Введение в современную теорию чисел: уч. пособие /Ю.И. Манин, А.А. Панчишкин. – М.: МЦНМО, 2009. -552 с.

References:

1 Chernov, V. (2007). Arifmeticheskiye metody sinteza bystrykh algoritmov diskretnykh ortogonal'nykh preobrazovaniy. Fismatlit. (p. 264).

2 Mallat, S., (2013), Course on High Dimensional Data Analysis, École Normale Supérieure. (p. 117).

3 Chakraborty, R. S., Scgwabe, P., & Solwaeth, J. (Eds.). (2015). Security, Privacy, and Applied Cryptography Engineering: 5th International Conference, SPACE 2015, Jaipur, India, October 3-7, 2015. Proceedings (Vol. 9354). Springer.

4 Ambrose, D. (2014). On Artin's Primitive Root Conjecture. Dissertation zur Erlangung des mathematisch-naturwissenschaftlichen Doctorgrades. In Doctor rerum naturalium (p. 169). der Georg-August-Universitat Gottingen.

5 Vostrov, G., & Opiata, R. (2018). Computer modeling of dynamic processes in analytic number theory. Electrotechnic and Computer Systems, (28), 240-247. https://doi.org/10.15276/eltecs.28.104.2018.29.

6 Caragiu, M., (2017). Sequential Experiments with Primes. Springer International Publishing (p. 290)

7 Lord, N. (2009). Experimental mathematics in action, by DH Bailey, JM Borwein, NJ Calkin, R. Girgensohn, DR Luke & VH Moll. Pp. 322. $49.00. 2007. ISBN 978 1 56881 271 7 (AK Peters). The Mathematical Gazette, 93(528), 564-566. https://doi.org/10.1017/S0025557200185511.

8 Murty, M. R. (2008). Problems in analytic number theory (Vol. 206). Springer Science & Business Media.

9 Abdymanapov, S., Turusbekova. U., Turginbayeva, A., & Altynbek, S. (2020) Research of Irreducible Norm Polynomials Special Type over a Field of Characteristic 2, IAENG International Journal of Applied Mathematics, 50(4), 777-782. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85098231325&partnerID=40&md5= 5949531a97827669e0d339b00af4b250

10 Moree, P. (1993). A note on Artin's conjecture. Simon Stevin, 67(3), 255-258.

11 Brüdern, J., & Godinho, H. (2002). On Artin's conjecture, II: pairs of additive forms. Proceedings of the London Mathematical Society, 84(3), 513-538. https: // doi.org/10.1112/S0024611502013588.

12 Manin, Yu., & Panchishkin, A. (2009). Vvedeniye v sovremennuyu teoriyu chisel. [Introduction to modern number theory]. Izd-vo MTSNMO (552 s.). Moskva